Homeland Security | Privacy Office

Protecting privacy while promoting transparency




HOW TO SAFEGUARD PERSONALLY IDENTIFIABLE INFORMATION

DHS employees and contractors are required to properly use, protect, and dispose of personally identifiable information (PII)

What is PII?

PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as that found on a business card. Other PII is ***sensitive PII***, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines.

Examples of sensitive PII include: Social Security number (SSN), alien registration number (A-Number), or biometric identifier (e.g., fingerprint, iris scan). Other data elements such as a driver's license number, financial information, citizenship or immigration status, or medical information, in conjunction with the identity of an individual, are also considered sensitive PII. In addition, the context of the PII may determine its sensitivity, such as a list of employees with poor performance ratings.

General Rules for Safeguarding <u>All</u> PII

- You must be authorized to collect PII.
- Minimize the collection, use and sharing of PII:
  - Don't create extra copies of PII before consulting your privacy point of contact.
  - Share PII only with other authorized personnel.
  - Minimize the use of SSNs.
- Dispose of PII properly: Consult your manager to obtain the retention schedule for your system.
  - Shred (do not recycle) paper containing PII.
  - Sanitize PII from computer drives and other electronic storage devices according to your component's information security standards or DHS 4300A Sensitive System Handbook.

General Rules for Safeguarding <u>Sensitive</u> PII

Privacy incidents occur primarily when employees fail to use the appropriate controls while sharing or using sensitive PII. A privacy incident is defined as the loss of control, compromise, or unauthorized disclosure, acquisition or access to PII, in physical or electronic form.

Follow these safeguards to avoid becoming a statistic

The following five media types account for 75% of all privacy incidents at DHS:

1. **EMAIL:** When emailing sensitive PII outside of the Department, save the sensitive PII in a separate document and encrypt it. See instructions below. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email. Some components require encryption when emailing sensitive PII within DHS, so check your policy. Never send sensitive PII to personal email accounts.

www.dhs.gov/privacy privacy@dhs.gov 703-235-0780

2 HARD COPY: Do not leave sensitive PII unattended on printers, fax machines, or copiers. Avoid faxing PII. Scan the document, encrypt and email it.

3 MAILING: Physically secure sensitive PII when in transit. Do not mail or courier sensitive PII on CDs, DVDs, hard drives, flash drives, USB drives, floppy disks, or other removable media unless the data is encrypted.

- Within DHS: Sensitive PII should be mailed in blue messenger envelopes furnished by your onsite DHS mailroom or courier. Verify that the recipient received the information.
- External mail: Seal sensitive PII in an opaque envelope or container, and mail using First Class or Priority Mail, or a commercial delivery service (e.g., DHL or FedEx).

4 MOBILE DEVICES: Sensitive PII may be saved, stored, or hosted only on DHS-authorized equipment (including contractor-owned equipment or a system that is approved to be used as a government system). Personally-owned computers may not be used to save, store, or host sensitive PII that is collected or maintained by DHS. Note: DHS issued or approved portable electronic devices (PEDs), such as laptops, USB drives, and external hard drives, must be encrypted. When traveling:

- Do not place a laptop or PED in checked luggage.
- If you must leave a laptop or PED in a car, lock it in the trunk so that it is out of sight.
- Avoid leaving a laptop or PED in a hotel room; if you must, lock it in a safe.

5 SHARED DRIVES: Only store sensitive PII on shared drives if access can be restricted to persons with proper authorization. Do this by password-protecting the document as well as the folder.

Instructions for encrypting a Word 2007 document:

1. In Word, click on the color wheel in the top left corner
2. Click on Prepare
3. Click on Encrypt Document
4. Type in a password
5. Click on Save

Report Privacy Incidents

You must report all privacy incidents, whether suspected or confirmed, to your supervisor *immediately.* If your supervisor is unavailable, or if there is a potential conflict of interest, report the incident to your Program Manager, Help Desk, or component privacy officer or privacy point of contact. To obtain more detailed guidelines on privacy incident reporting, download the *Privacy Incident Handling Guidance* on DHS Connect.

For More Information

To obtain more detailed guidelines on the safe handling of sensitive PII, download the *Handbook for Safeguarding Sensitive PII* on DHS Connect, or email *privacy@dhs.gov* to request a copy.

August 2010